UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,524	03/31/2004	Kenneth E. Nicholas	200313756-1	6916

22879 7590 11/08/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
11/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,524	NICHOLAS, KENNETH E.	
	Examiner	Art Unit	
	Devin Almeida	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 10/24/2007.

Response to Arguments

Applicant's arguments with respect to Copper et al have been fully considered but they are not persuasive. Copper clearly teaches that a biometric such as a retinal scanner (eye scanner); finger print scanner; thumb print scanner; DNA scanner; and other type of biometrics scanning mechanism is used to choose the encrypting key for a device in paragraph 0077.

Applicant's arguments with respect to Balfanz et al have been fully considered but they are not persuasive. Balfanz clearly teaches that a biometric information is used to generate keys that are used in group communication in column 5 lines 60-67.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5, 7, 10, 14, 16, 18, 19, 21, 23, 26, 30, 34 and 36 are rejected under 35 U.S.C. 102(e) as being anticipated by Cooper et al (2002/0029350). With respect to

claim 1, a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user (see paragraph 0075 i.e. a message received into a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)); and a configuration module adapted to automatically select a communication network configuration setting for a device based on the received biometric data (see paragraph 0075-0077).

With respect to claim 2, comprising relational data accessible by the configuration module for correlating the received biometric data to the selected network configuration setting (see paragraph 0075 – 0077).

With respect to claim 3. The system of claim 1, wherein the selected network configuration setting comprises at least one of the group consisting of a local area network (LAN) configuration setting, a wide area network (WAN) configuration setting, a personal area network (PAN) configuration setting and a virtual private network (VPN) configuration setting (see paragraph 0077 i.e. VPN).

With respect to claim 5, wherein the configuration module is adapted to compare the received biometric data to stored biometric data to select the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 7, wherein the biometric data comprises at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (see paragraph 0075 i.e. a message received into

a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)).

With respect to claim 10, wherein the configuration module is adapted to request from the user a particular biometric to associate with the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 14, comprising: means for receiving biometric data from a user (see paragraph 0075 i.e. a message received into a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)); and means for automatically selecting a communication network configuration setting for a device based on the received biometric data (see paragraph 0075-0077 i.e. VPN).

With respect to claim 16, further comprising means for comparing the received biometric data to stored biometric data to select the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 18, further comprising means for requesting from the user a particular biometric to associate with the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 19, comprising: receiving biometric data from a user (see paragraph 0075 i.e. a message received into a system containing verified biometric data

(finger print, face recognition, eye/retina recognition, voice recognition etc.)); and automatically selecting a communication network configuration setting for a device based on the received biometric data (see paragraph 0075-0077 i.e. VPN).

With respect to claim 21, further comprising comparing the received biometric data to stored biometric data to select the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 23, wherein receiving biometric data comprises receiving at least one of the group consisting of fingerprint scan biometric data, voice scan biometric data, facial feature biometric data, and eye scan biometric data (see paragraph 0075 i.e. a message received into a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)).

With respect to claim 26, further comprising requesting from the user a particular biometric to associate with the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well).

With respect to claim 30, comprising: a biometric sensor module adapted to receive biometric data associated with a user of a device (see paragraph 0075 i.e. a message received into a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)); and a configuration module adapted to associate a communication network configuration setting for the device with the biometric data (see paragraph 0075-0077 i.e. VPN).

With respect to claim 34, wherein the configuration module is adapted to associate with the network configuration setting at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (see paragraph 0075 i.e. a message received into a system containing verified biometric data (finger print, face recognition, eye/retina recognition, voice recognition etc.)).

With respect to claim 36, wherein the configuration module is adapted to request from the user a particular biometric to associate with the network configuration setting (see paragraph 0075 – 0077 i.e. The scanned image containing biometrics information will also be saved along with the Session and Public Encryption Keys as well)

Claims 1, 2, 3, 4, 6-9, 11, 14, 17, 19, 22-25, 27, 30-32, 34, and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Balfanz et al (U.S. 7,185,199). With respect to claim 1, a biometric configuration management system, comprising: a biometric sensor module for receiving biometric data associated with a user (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor); and a configuration module adapted to automatically select a communication network configuration setting for a device based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 2, further comprising relational data accessible by the configuration module for correlating the received biometric data to the selected network configuration setting (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 3, wherein the selected network configuration setting comprises at least one of the group consisting of a local area network (LAN) configuration setting, a wide area network (WAN) configuration setting, a personal area network (PAN) configuration setting and a virtual private network (VPN) configuration setting (see Balfanz column 3 lines 5-24).

With respect to claim 4, wherein the configuration module is adapted to automatically switch the device to the selected network configuration setting from another network configuration setting based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 6, wherein the configuration module is adapted to display an interface to the user identifying a particular biometric associated with the network configuration setting (see column 5 line 57 – column 6 line 8).

With respect to claim 7, wherein the biometric data comprises at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (see column 5 line 57 – column 6 line 8).

With respect to claim 8, wherein the configuration module is adapted to receive a selection from the user of the network configuration setting to associate with the biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 9, wherein the configuration module is adapted to display an interface to the user identifying registered biometrics (see column 5 line 57 – column 6 line 8).

With respect to claim 11, wherein the selected network configuration setting comprises a wireless network configuration setting (see Balfanz column 3 lines 5-24).

With respect to claim 14, a biometric configuration management system, comprising: means for receiving biometric data from a user (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor); and means for automatically selecting a communication network configuration setting for a device based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 17, further comprising means for automatically switching the device to the selected network configuration setting from another network configuration setting based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 19, a biometric configuration management method, comprising: receiving biometric data from a user (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor); and automatically selecting a communication network configuration setting for a device based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 22, further comprising automatically switching the device to the selected network configuration setting from another network configuration setting based on the received biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 23, wherein receiving biometric data comprises receiving at least one of the group consisting of fingerprint scan biometric data, voice scan biometric

data, facial feature biometric data, and eye scan biometric data (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor).

With respect to claim 24, further comprising requesting a selection from the user of the network configuration setting to associate with the biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 25, further comprising displaying to the user biometrics registered with particular network configuration settings (see column 5 line 57 – column 6 line 8).

With respect to claim 27, wherein automatically selecting a communication network configuration setting comprises automatically selecting a wireless communication network configuration setting (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35, column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 30, a biometric configuration management system, comprising: a biometric sensor module adapted to receive biometric data associated with a user of a device (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor); and a configuration module adapted to associate a communication network configuration setting for the device with the biometric data (see Balfanz column

5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication).

With respect to claim 31, wherein the configuration module is adapted to receive a selection from the user of the network configuration setting to associate with the biometric data(see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

With respect to claim 32, wherein the configuration module is adapted to display to the user an interface for associating a particular biometric with the network configuration setting (see column 5 line 57 – column 6 line 8).

With respect to claim 34, wherein the configuration module is adapted to associate with the network configuration setting at least one of the group consisting of a fingerprint scan biometric, a voice scan biometric, a facial feature biometric, and an eye scan biometric (See Balfanz figure 2 block 208 and column 1 line 60-67 i.e. fingerprint sensor).

With respect to claim 37, wherein the configuration module is adapted to associate a wireless communication network configuration setting for the device with the biometric data (see Balfanz column 5 line 64-66, i.e. the biometric information is used to generate keys, column 1 lines 34-35 and column column 2 lines 62-64 i.e. securing

communication over a communication medium, keys are used in group communication and column 3 lines 5-24).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 15, 16, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balfanz et al (U.S. 7,185,199) in view of Raaf (DE 198 37 642 C1). With respect to claim 5, Balfanz does not teach wherein the configuration module is adapted to compare the received biometric data to stored biometric data to select the network configuration setting. Raaf teaches wherein the configuration module is adapted to compare the received biometric data to stored biometric data to select the network configuration setting (see Raaf page 3 as a function of the results of the comparison when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe' the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have stored information about a fingerprint so that when the fingerprint is input it can trigger an action to be taken when that fingerprint in input (See page 3 and 4). Therefore one would have been motivated to have stored biometric data

to trigger an action to select the network configuration setting based on the biometric data input.

With respect to claim 15, further comprising means for identifying to the user a particular biometric associated with the network configuration setting (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 16, further comprising means for comparing the received biometric data to stored biometric data to select the network configuration setting (see Raaf page 3 as a function of the results of the comparison when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe' the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered).

With respect to claim 20. The method of claim 19, further comprising identifying to the user a particular biometric associated with the network configuration setting (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure).

With respect to claim 21, further comprising comparing the received biometric data to stored biometric data to select the network configuration setting (see Raaf page 3 as a function of the results of the comparison when the stored fingerprint information 'f4' is similar to the determined fingerprint information 'fe' the control procedure 'stp4' associated with this stored fingerprint information 'f4' is triggered).

Claims 33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balfanz et al (U.S. 7,185,199) in view of Raaf (DE 198 37 642 C1) in further view of Sudo (U.S. 5,987,336). Balfanz teach everything with respect to claim 30 above but with respect to claim 33 he does not teach wherein the configuration module is adapted to display a plurality of available network configuration settings to the user for associating with the biometric data. Raaf teach network configuration settings to the user for associating with the biometric (see page 2 i.e. different pieces of fingerprint information corresponding to one finger each of various persons is stored each piece of information being associated with a control procedure). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have stored information about a fingerprint associated with a control procedure so that when the fingerprint is input it can trigger an action to be taken (See Raaf page 3 and 4). Therefore one would have been motivated to have stored biometric data associated with a network configuration setting based so that when the biometric data input it triggers an action to be taken. Neither Balfanz nor Raaf teach display a plurality of available network configuration settings to the user. Sudo teaches displaying a plurality of available network configuration settings to the user (see column 15 line 61 – column 16 line 7). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have display the available network to help the user select a network to use (see Sudo column 15 line 61 – column 16 line 7). Therefore one would have been motivated to have displayed available network

With respect to claim 35, wherein the configuration module is adapted to display to the user biometrics registered with particular network configuration settings (See Raaf page 3 and 4 and Sudo column 15 line 61 – column 16 line 7).

Claims 12, 13, 28, 29, 38, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balfanz et al (U.S. 7,185,199) in view of Topping (2004/0151353). Balfanz teaches everything with respect to claim 1, 29, and 30 above but with respect to claims 13, 29 and 39 he does not teach wherein the received biometric data comprises a plurality of sequentially input biometrics. Topping teaches wherein the received biometric data comprises a plurality of sequentially input biometrics (see Topping paragraph 0017 and 0032). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have requires several fingerprints to be entered in a particular sequence to further increase system security (see Topping paragraph 0017). Therefore one would have been motivated to have input a plurality of sequentially input biometrics to increase system security.

With respect to claim 12, 28 and 38, wherein the received biometric data comprises a plurality of simultaneously input biometrics (see Topping paragraph claim 13).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
10/4/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100